Alder Grange School
Third Party Data Handling Policy

GCSE POD User Data

Mandatory Data

Student data	Why
MIS ID	Used as a unique identifier with single sign on for ADFS and Moodle. Prevents duplicate records being created.
Date of birth	Combined with additional information, creates a unique identifier for self-activation of accounts. Used when a student needs to recover a lost/forgotten password. Also used in reporting for staff members.
Surname	Combined with additional information, creates a unique identifier for self-activation of accounts. Used when a student needs to recover a lost/forgotten password. Also used in reporting for staff members and to set assignments and monitor usage.
Forename	Combined with additional information, creates a unique identifier for self-activation of accounts. Used when a student needs to recover a lost/forgotten password. Also used in reporting for staff members and to set assignments and monitor usage.
Admission number	Used as a unique identifier to support the movement of data and prevent duplicates (for example if a school chooses to move MIS system).

Staff data	Why
Title	Used to set naming conventions.
Surname (preferred)	Used to identify staff members for reporting.
Forename (preferred)	Used to identify staff members for reporting.
Main work email	Used to identify a staff member on activation of their account. Used in reporting as an identifier and can be used to reset lost/forgotten passwords. Can be used as an opt-in only notification system.
Primary email address	Used when work email data field is unpopulated. See above.
Teaching/non-teaching staff	Used to differentiate between teaching and non-teaching staff.
Date of leaving	Used to make a decision about whether to import data about the particular staff member.
Role text	Used to identify staff by their job roles.

Data Type	Why
Student data extended	
Pupil premium indicator	Used to help school measure impact of key demographics.
Gifted	Used to help school measure impact of key demographics.
English as an additional language	Used to help school measure impact of key demographics.
Gender	Used by staff members to analyse usage.
Primary email address	Used as a unique identifier for certain integrations (e.g. Office 365 and Firefly VLE).
Unique pupil number	Used as a unique identifier for Moodle, Frog and Realsmart VLE integration. Also used if a school creates custom groups via CSV upload.
Staff Code	Used as a unique identifier for single sign-on integration with Frog and Realsmart.

Group data	Why
Group name	Identifies the name of a group stored in the school's MIS so that staff members can report on groupings of students. Used to set assignments for particular groups.
Group type	Identifies group type to help identification for user.
Group ID	Unique identifier for a group.
Registration group	Identifies registration group types to help identification for the user.
Year Group	Identifies year group types to help identification for the user.
Class name	Identifies class group types to help identification for the user.
Subject name	Identifies a subject to append to class group and teacher information.

Parent Mail

In order to carry out these services, we obtain (either from the Customer and/or from you directly) and process the following information:

Data Subject (Who) Data Category (What) Description
Pupil \ Student Forename This is the forename of the pupil.
Pupil \ Student Surname This is the surname of the pupil.
Pupil \ Student Known as This is the name that the pupil is known as.
Pupil \ Student DOB This is the date of birth of the pupil.
Pupil \ Student Gender This is the pupil's gender
Pupil \ Student Groups Registration group (if any), year, other groups
Pupil \ Student Salutation This is the pupil's salutation.
Pupil \ Student Dietary Requirements This is the pupil's special dietary requirements
Pupil \ Student Postal Address The student's postal address
Pupil \ Student Identifiers Roll/Admission number, UPN, management system identifier
Pupil \ Student Meal Selections and spend history this is a history of a pupil's meal selections and spends for school meals or non-meal-related items, including free school meals
Pupil \ Student Trip information Trip details collected from parents, e.g. emergency contacts, medical details, dietary requirements, doctor's contact, EHIC and Passport
Parent's \ Contacts Title This is the contact's title (Mr, Mrs, Ms, etc).
Parent's \ Contacts Forename This is the contact's forename.
Parent's \ Contacts Surname This is the contact's surname.
Parent's \ Contacts Authentication data Username and password, single-sign-or multi-factor-authentication tokens
Parent's \ Contacts Gender The contact's gender (Salutation)
Parent's \ Contacts House Name The text entered as the contact's house name.
Parent's \ Contacts Street the text entered as the contact's street.
Parent's \ Contacts Locality The text entered as the contact's locality.
Parents \ Contacts Town The text entered as the contact's town.
Parent's \ Contacts Postcode The text entered as the contact's post code.
Parent's \ Contacts Day Telephone The contact's daytime telephone number.
Parents \ Contacts Home Telephone The contact's home telephone number. Parent's \ Contacts Mobile Telephone This is the contact's mobile telephone number used to receive alerts from Parentpay and for school communications
Parents \ Contacts Email This is the contact's E-mail address used to receive communications from Parentpay and for school communications.
Parent's \ Contacts Payment History and balances this is the contact's history of payment transactions, including reversals, refunds and withdrawals of funds.
Parents \ Contacts Payment card details Payment card details are captured and passed to a 3rd party for authorisation.
Parent's \ Contacts Other This is the contact's alternative communication method.
Parents \ Contacts In-app messages Messages sent from parents to school within the ParentPay application
Parent's \ Contacts Trouble ticket data when users submit trouble ticket information, this gets stored.
Parent's \ Contacts Shop information ParentPay can be used as a payment page from externally or internally hosted shop systems. This the information captured as part of that ("shopping basket").
Parents \ Contacts Browser Details IP address, cookies, browser information
Parent's \ Contacts Scottish UPRN For users in Scotland who sign up via MyGovScot
School Staff Title This is the staff member's title (Mr, Mrs, Ms, etc.).
School Staff Forename This is the staff member's forename.
School Staff Surname This is the staff member's surname.

School Staff Gender The staff member’s gender
Website Access IP Address The network address of your device or internet connection
Website Access Browser Type and Version The type of Web Browser your device is using
Website Access Cookies Special records in your browser to help the website operate
Website Access Web Analytics Generalised information about browsing behaviour and page statistics

Parent Pay

How we process your personal information

We use your personal information, and some of our employees have access to such information, only to the extent required to carry out the services for you and on behalf of the Customer.

Why Parent Pay use your personal information

The PPL payment solutions, catering systems and communication platforms ("PPL Products and Services"), which are marketed in the UK under the ParentPay, Schoolcomms and Cypad brands, are provided to schools and their parents governed by a contract between us and the schools, Multi-Academy Trust or a Local Education Authority ("ParentPay Customer"), and also the Terms and Conditions that you agree with when you sign up ("ParentPay User").

We process your personal data for the following purposes:

- To provide you with the service activated and registered for the verification of your identity where required.
- For the prevention and detection of crime, fraud and anti-money laundering.
- For the ongoing administration of the service
- To allow us to improve the products and services we offer to our customers.
- For research and statistical analysis including payment and usage patterns

We only use the data in an anonymized manner when we use your data for this purpose.

- To enable us to comply with our legal and regulatory obligations.
- To offer new products and services to you which are relevant and appropriate, and only to the extent that would be reasonably expected.

If we plan to introduce further processes for the use of your information, we will provide information about that purpose prior to such processing.

Hegerty Math's

Hegartymaths has the following permissions approved to access your school data. Student Groups, Classes & Subjects.

Required Permissions:

The following permissions are required by Hegartymaths to perform as expected:

View student data
View student identifier data
View student UPN data
View student local UPN data
View former UPN data
View student admission number data
View student UPI data
View student MIS id data
View student title data
View student initials data
View student surname data
View student forename data
View student middle names data
View student legal surname data
View student legal forename data
View student gender data
View student date of birth data
View student education details data
View student current NC year data
View student leaving date data

BKSB

BKSB Limited are committed to ensuring the security of our customer's data and have taken great efforts to implement technical and organisational measures to ensure data is secure from unauthorised access. With the planned introduction of the new GDPR regulations in May 2018, this document outlines some of the actions and measures we have put in place to ensure compliance for the bksbLIVE 2 assessment and learning platform.

1. **Appointed a data protection officer.** Our data protection officer is Ian Lilliman and can be contacted either by telephone (01623 413333) or by email at dpo@bksb.co.uk.
2. **Carried out a DPIA and identified our lawful basis.** As per the requirements of organisations that process large volumes of data, we have carried out a data protection impact assessment and documented the findings. Where we have used legitimate interest as our lawful basis, we have carried out a 3-part legitimate interest test to ensure the processing is a) necessary for the purpose, b) be reasonably expected by the data subject, and c) the interests of bksb Limited do not override the interest of data subjects.
3. **Updated our Terms & Conditions and Privacy/cookie policy.** We have created updated versions of the aforementioned documents to reflect the requirements to explain how we use your data, the lawful basis and the rights of data subjects. **These documents will be updated on the LIVE 2 platform in May.**
4. **Breach reporting and data subject access requests.** In line with the requirements of GDPR Article 33 (2), we have implemented new breach reporting and data subject access request policies together with the relevant forms.
5. **Implementation of ISO27001 (information security).** We are currently in the final stages of achieving the ISO27001 accreditation.
6. **The following information provides an insight into some of the measures we have implemented with regards to our compliance with Article 32 (Security of processing) of GDPR.**
7. **Information Commissioner's Office Certificate.** bksb limited is registered with the Information Commissioner's Office under the registration reference: ZA042176.

a) Compliance with Article 32 (Security of processing), para 1 of GDPR

i. Consideration of pseudonymisation and encryption. Passwords are encrypted for security reasons. Passwords are not visible to the Processor nor any of its sub-contractors (such as Amazon AWS) engaged in the delivery, management or monitoring of the system. Connection between you and bksb Limited systems are encrypted using https protocol. We hold 3 months' worth of backups in encrypted format (in a separate UK-based location) in the event of a need to restore an account.

ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services. Our systems, policies and procedures are regularly reviewed in accordance with the ISO27001 (Information Security) standards. We use an Amazon-approved third party to a) monitor our systems 24/7/365 for issues that may cause a disruption to service and b) manage the timely deployment of server patches and other related updates.

iii. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. bksb Limited maintains a Business Continuity Plan to safeguard against events which may cause disruption to its business and the services it delivers. This is regularly reviewed in line with our (ISO27001) quality management system.

iv. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing. bksb Limited carry out penetration tests every 3 months to determine the effectiveness of the security measures we have in place and this feeds back into our (ISO27001) quality management processes. All other security policies and procedures are reviewed and audited every 12 months in accordance with our quality management framework.

b) Compliance with Article 32 (Security of processing), para 2 of GDPR

i. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed. Change management processes in place to control changes to the system, anti-virus and firewall protection in place to prevent against malicious web requests or other unusual activity, multi-factor authentication to prevent unauthorised access, backups are encrypted. Access to key systems also restricted via IP address. System monitored 24/7/365 by Amazon-approved third party for issues that may cause a disruption to service. Daily (encrypted) backups to alternate UK-based location.

c) Compliance with Article 32 (Security of processing), para 3 of GDPR

i. Adherence to an approved code of conduct referred to in Article 40 (GDPR) or an approved certification mechanism as referred to in Article 42 (GDPR) may be used as an element by which to demonstrate compliance with the requirements set out in para 1 of GDPR – see above. bksb Limited are working towards acquiring the ISO27001 (Information Security) accreditation.

d) Compliance with Article 32, para 4 of GDPR

i. The Processor to ensure that anyone acting on their behalf does not process any of the Data unless following instructions from the controller unless they are required to do so under English law. Company data protection, IT & Information policies in place. All staff are DBS checked and have confidentiality clauses in their employment contracts. System access controlled through permissions and multi-factor authentication.

LCR Limited – Quick Dine Cashless Catering

Our Responsibility to Customers.

LCR is working to meet the requirements of the GDPR legislation. Our promise to customers and partners:

- We only manage data with agreement of the data controller.
- We will use and continue to update safeguards around data handling.
- We will implement confidentiality requirements on its personnel.
- We work to help the controller meet the rights of the data subjects.

For further detail and information on GDPR legislation – please visit the UK Information Commissioner's Office website.

What LCR Limited is already doing:

Data processing with partners

LCR uses some 3rd party systems to fulfil our data processing duties requested by Local Authority & School Clients

This includes: the storage and use of personal information handed to us by the school e.g. through 3rd parties such as; Capita, ParentPay, Tucasi, ParentMail Schoolcomms. Schools are entitled to know which 3rd parties we use, and what data is being shared.

LCR will assess its 3rd parties to ensure valid compliance with any changing legislation.

Contractual changes

LCR will be revising our existing contracts with schools to reflect the requirements of the new legislation.

Breach notification

In the event of a data breach LCR will follow the Information Commissioner's Office guidelines LCR LIMITED- QUICKDINE CASHLESS & GDPR - MAY 2018 2

Questions about data we hold

LCR do not transfer any data to countries outside of the EEA. The cloud providers that we work with guarantee data is only processed in the EEA, or that they explicitly abide by the regulation. Please report any data protection related concerns to (email) dataprotection@lcrltd.com

Security

Security of data is essential. LCR use protection measures and carry out regular audits to assess our security practices.

Helping Your School Demonstrate Compliance

Under the data protection law, controllers (i.e. the schools) will need to demonstrate their compliance, which in turn means they need to assess the compliance of all of their service suppliers. LCR is adopting enhanced procedures and policies which will comply with GDPR requirements.